I, Christopher J. Kefalas, Special Agent, Bureau of Alcohol, Tobacco, Firearms & Explosives, being duly sworn, states:

1. I have been employed as a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), United States Department of Justice and have been so employed since 2015. I am a graduate of Criminal Investigator Training Program at the Federal Law Enforcement Training Center and Special Agent Basic Training at the ATF National Academy both in Glynco, Georgia. I received a master's degree in Criminal Justice from Northeastern University in 2014 and a bachelor's degree in Criminology from Stonehill College in 2012. I am responsible for the investigation of violations of and the enforcement of federal firearms laws. I am presently assigned to the Bridgewater Field Office, where I am one of a group of Special Agents who work with state and local law enforcement to uncover violations of laws specifically related to firearms trafficking, firearms possession by prohibited persons, and use of firearms in furtherance of drug trafficking crimes, in southeastern Massachusetts. I personally participated in the investigation of violations of federal law by **Chiweze IHUNWO** during the course of this investigation.

2. During my tenure with ATF, I have participated in dozens of investigations and have had training in various aspects of firearms' investigations. I have conducted surveillance, worked with confidential informants, participated in investigations using court-authorized interception of wire and electronic communications. During my law enforcement career, I have also participated in the preparation and execution of arrest warrants and search warrants.

3. I have personally participated in the investigation of **Chiweze IHUNWO**, who was born in 1996, since approximately April 2020.

4. I am familiar with the facts and circumstances of this investigation based upon: (a) my personal knowledge and involvement in the investigation; (b) my discussions with fellow agents and officers who assisted in the investigation; and (c) my review of various records and documents. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the requested warrant, I have not set forth every fact learned during the course of the investigation.

5. I am submitting this affidavit in support of an application for the issuance of a Search Warrant to be executed at 60 Rowley Street in Providence, Rhode Island (the "Target Location"), as described in Attachment A. As set forth below, the evidence demonstrates that **Chiweze IHUNWO** has been living at the Target Location.

6. As described more fully below, there is probable cause to believe that evidence of IHUNWO's violation of Title 18 of the United States Code 922(a) ("the Target Offense"), engaging in the business of dealing in firearms without a license, and that evidence, fruits, and instrumentalities of the Target Offense, as described in Attachment B, exist at the Target Location.

The Target Location

7. The Target Location (60 Rowley Street, Providence, RI) is a single story residential ranch with yellow wood shingles and maroon accents and shutters. The driveway associated with 60 Rowley Street is on the right side of the residence. The front door of the residence is accessible via Rowley Street while there is a side door to the residence accessible by the referenced driveway. The residence also has a back bulkhead which faces outward toward the backyard. The property is believed to be owned by Frantz Cadet.

8. A Honda sedan (Rhode Island license plate number WX209) is registered to Janessa Schobel at the Target Location. IHUNWO is known to have operated this vehicle based upon observations made by Randolph (Massachusetts) Police Department Detective Richard Brewer and observations made by this Special Agent.

9. On September 27, 2020, the Randolph Police Department conducted surveillance at the Target Location. On this date, the Randolph Police Department observed the Honda sedan (RI Reg. WX209) parked in the driveway of the residence. The Randolph Police Department also observed a silver Honda Accord (Massachusetts license plate number 1SRR31) parked on the street; this vehicle is registered to IHUNWO's father at 50 N. Lillian Street in Randolph, Massachusetts. The Randolph Police Department also observed other vehicles, but their license plates could not be observed due to obstructions.

10. On November 2, 2020, I conducted surveillance of 60 Rowley Street in Providence, Rhode Island. Multiple vehicles were present at the target address, including a silver pickup truck, silver Nissan sedan, a black Jeep, and the Honda (WX209).

11. According to records provided by T-Mobile, telephone 617-818-8654 (the "Target Telephone") is subscribed to IHUNWO with an address of 50 Lillian St. N, Randolph, Massachusetts.

12. Beginning on or around October 30, 2020, pursuant to a federal search warrant signed by the Honorable Judith G. Dein, U.S. Magistrate Judge, District of Massachusetts (20-5365-mj-JGD), T-Mobile has been providing ATF with location data points indicating the approximate location of the Target Telephone ("ping" data). According to the ping location data, the Target Telephone was nearby the Target Location at various recent periods of time, including

overnight from October 30, 2020 – October 31, 2020, the early morning of November 1, 2020, and overnight from November 1, 2020 – November 2, 2020.

13. On November 3, 2020, I conducted surveillance of 60 Rowley Street in Providence, Rhode Island and observed the Honda (WX209) to be present at the target address. At this same time, the ping data showed the Target Telephone to be in the area of the Target Location. On this same date, IHUNWO posted on the Instagram account "Weezoskolo" a photograph pointing a firearm at the camera while believed to be in a vehicle and later posted, "Anyone need food? (Bang/Flash emoticon)(Eyes emoticon)." Based on the training and experience of this Special Agent, I know "food" to be a commonly utilized term when talking about ammunition.

14. On November 4, 2020, the ATF and Randolph Police Department conducted surveillance of IHUNWO in Brockton, Massachusetts. Investigators observed IHUNWO exit Sodade's Barbershop on Main Street in Brockton, Massachusetts and enter the Honda (WX209). The ping data then showed the Target Telephone to return to the area of the Target Location that evening.

15. On November 5, 2020, at approximately 7:00 p.m., the Rhode Island State Police ("RISP") arrested IHUNWO at the Target Location in connection with allegations that he threw a water bottle at another vehicle while operating the Honda (WX209). The IHUNWO Instagram account posted live videos during the transport of the arrest and in the booking area while claiming he had hid his cellular telephone in his sock. On this same day, the ping data showed the Target Telephone to be at or around both the Target Location and the RISP Lincoln Barracks at the pertinent times.

16. Between November 7, 2020 – November 9, 2020, RISP has observed IHUNWO coming and going from the Target Location at varying times of the day and night. For example, on November 9, 2020, at approximately 10:30 a.m., RISP observed IHUNWO exit the Target Location and enter the driver's seat of the Honda (WX209) with a female who entered the passenger seat. RISP then observed the Honda leave the area. Based on the ping data, the facts developed during the investigation showing IHUNWO to be the user of the Target Telephone, IHUNWO's recent arrest, and my training and experience, I believe that IHUNWO has recently been living at the Target Location.

Evidence of Gun Trafficking

17. On September 30, 2020, search warrants were issued in case number 20-mj-5341-JGD, 20-mj-5342-JGD, 20-mj-5343- JGD, and 20-mj-5344-JGD for certain social media accounts associated with IHUNWO. The affidavit utilized in these search warrants is attached to this affidavit as Exhibit 1 and is hereby incorporated by reference.

18. On October 28, 2020, search warrants were issued in case number 20-5365-JGD and 20-5366-JGD for historical cell site data and ping information associated with the Target Telephone. The affidavit utilized in these search warrants is attached to this affidavit as Exhibit 2 and is hereby incorporated by reference.

19. As set forth in Exhibits 1 and 2, there is significant evidence that IHUNWO has been engaged in the unlicensed dealing in firearms. Among this evidence is the following:

a. Randolph Police Department determined that IHUNWO was posting photographs of multiple firearms on social media along with language consistent with an intention to sell firearms and ammunition. Exhibit 1, ¶¶ 6-10.

b. ATF researched serial numbers of a shotgun and a Glock that were visible in photographs posted on IHUNWO's Instagram profile. ATF learned that each of these firearms had been purchased by PERSON 1, a resident of North Carolina. *Id.*, ¶ 11.

c. In August 2020, IHUNWO posted numerous photographs of firearms to a social media account, including one showing IHUNWO holding a rifle. That same day, a posting to IHUNWO's account included a video geotagged to a North Carolina location at or near the residence of PERSON 1. Other postings around this time are indicative of IHUNWO seeking to sell firearms (*e.g.*, reference to "lowball" offers; reference to contact "to do business;" "If you cant afford what I'm selling then it aint for you"). *Id.*, ¶¶ 17-19.

d. ATF agents interviewed PERSON 1, who indicated that he knew someone named "Weez" who used the Target Telephone. PERSON 1 indicated that "Weez" (referred to hereafter as IHUNWO) had sent money to PERSON 1 for firearms that IHUNWO would pick up on trips to North Carolina. *Id.* ¶¶ 27-28.

e. A review of messages found on PERSON 1's phone reveals a large volume of communications concerning IHUNWO's efforts to acquire firearms, concerning pricing for these firearms, and/or concerning IHUNWO's firearm customers. Exhibit 1, ¶ 18. Based on these communications, and my training and experience, I know that IHUNWO engaged in a longstanding pattern of acquiring firearms from North Carolina and of offering firearms for resale.

f. IHUNWO has no Federal Firearms License and is thus not licensed to engage in the dealing of firearms. Exhibit 1, ¶ 39.

20. On or about November 3, 2020, Facebook produced records for the Facebook and Instagram accounts of IHUNWO. An initial review of these records revealed further evidence of IHUNWO's firearms possession and firearms trafficking. For example, on April 22, 2020, the Instagram account of IHUNWO, Instagram user "Weezoskolo," sent a message to Instagram user "elianchoo" which contained a photograph of a black semi-automatic pistol with a Smith & Wesson slide, Surefire under barrel light, and a Burris red dot rear mounted sight with text which stated, "Thats my blick just modified."

21. On July 14, 2020, Instagram user "Weezoskolo" messaged Instagram user "otmbclumz" and stated, "But you dont know me to be saying you putting in more work ask Donnie bout me I put in work out here fr and I be moving the sticks I hit you on some shit like n****s need that we got that." Based on the training and experience of this Special Agent, I know "sticks" to be a commonly utilized term to describe firearms.

22. I believe, based on my training and experience and the facts developed during this investigation that IHUNWO continues to be involved with firearms dealing. For example, on November 1, 2020, Randolph Police Department Detective Richard Brewer observed that the Instagram account of IHUNWO (Instagram username "weezoskolo") posted a story which stated, "Best part about being the plug you get the good s**t first (Ghost Emoticon) (Flash/Bang Emoticon)." Based upon the training and experience of this Special Agent, a "plug" is common terminology for a source of supply for firearms or narcotics. Based upon the totality of this investigation, this Special Agent believes IHUNWO is referencing being a source of supply for firearms and having first selection on quality firearms.

Evidence Likely to be Found at Target Location

23. Based on my training and experience as an ATF Special Agent, I know that individuals who own and possess firearms frequently possess and maintain them for long periods of time because firearms are somewhat expensive and do not easily wear out. In my training and experience, personal firearms are unlike narcotics or currency, which are often used or exchanged soon after being obtained. Firearms are similar to tools that a person buys and maintains. Persons who own and possess firearms generally keep them in their residences unless carrying in their possession outside of the residence. It has also been my experience that persons maintain firearms along with ammunition in a convenient and safe location to afford ease of access. Based upon the messages obtained between the Target Telephone and the telephone of PERSON 1, I believe that IHUNWO consistently has one or more firearms in his possession due to IHUNWO's description of not "lacking." In the training and experience of this Special Agent, to be "lacking" is common verbiage indicating to be without a firearm.

24. Based on my training and experience, I also know that those involved in the trafficking and sale of firearms often maintain firearms and ammunition while in the process of arranging sales for the firearms and ammunition. Those engaged in the business of selling firearms also frequently maintain records such as ledgers, receipts, and other documentation of the sale of the firearms and ammunition. In this instance, I also know that IHUNWO was attempting to sell firearms accessories and equipment, such as laser sighting systems. Based upon my training and experience, I know that those engaged in the sale of firearms often possess firearms parts, accessories, and equipment to either sell or to maintain the firearms they possess.

25. Based on my training and experience, I know that individuals engaged in the business of selling firearms frequently use electronic devices (including smartphones, tablets, or computers) in furtherance of that business, including to communicate with suppliers, potential suppliers, customers, and potential customers; to research firearm specifications, availability, and pricing; to make arrangements for the acquisition, transportation, or sale of firearms; and to track revenue and expenditures.

26. Based on my training and experience, I also know that individuals who own and possess cellular telephones normally possess and maintain them for reasonably long periods of time because they are somewhat expensive, can often be subject to long-term contracts that contain substantial penalties for early termination, and do not easily wear out. In addition, most modern phones (generally referred to as “smartphones”) afford access to the internet and to social websites like Facebook, Instagram, and Snapchat, have camera capabilities, and many users tend to store photos in their cell phones which are most often maintained by the user on his person or in his residence when not outside.

27. Based on my training and experience, I know that individuals often use multiple devices – including smartphones, tablets, laptop computers, and/or desktop computers – to access social media accounts such as Facebook, Instagram, and Snapchat.

Search of Computer Equipment

28. Based on the reflected above, and my training and experience, I know that IHUNWO has used one or more electronic devices to commit, and/or in connection with, the Target Offense.

29. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly create, receive, send, and/or store records of the type described in Attachment B in computer hardware, computer software, smartphones, and/or storage media.

30. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which

might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a

digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

31. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of

> computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

32. The TARGET LOCATION may contain computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

CONCLUSION

33. Based on the foregoing, and based on my training and experience, I believe that there is probable cause to believe that the premises located at 60 Rowley Street in Providence, Rhode Island, as described in Attachment A, presently contain evidence, contraband, and/or the fruits of the Target Offense, as described in Attachment B.

Sworn to under the pains and penalties of perjury,

Christopher J. Kefalas
Special Agent, ATF

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by **telephone**.

_____	_____
Date	*Judge's signature*
_____	Lincoln D. Almond, US Magistrate Judge
City and State	*Printed name and title*

ATTACHMENT A
Property to be Searched

The interior of the residence at 60 Rowley Street Providence, Rhode Island 02909. This residence is described as a yellow, single story, single family ranch home. This house has maroon colored shutters and roofline, and has white trim around the windows. The residence has a driveway to the right side of the house. The front door is accessible via Rowley Street while the side door is accessible via the aforementioned driveway. The residence is located on the West side of Rowley Street and can be located by driving North on Rowley Street from Chalkstone Avenue. 60 Rowley Street is on the left side of the street (West) midway on the dead end street.

ATTACHMENT B
Items to be Seized

1. All records (in whatever form) and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 922(a)(1), including but not limited to the following:

A. Records relating to the possession, acquisition, purchase, storage, transportation, use, distribution, or sale of any firearm, ammunition, firearm parts and/or accessories.

B. Firearms, ammunition, or firearm parts or accessories.

C. Firearm boxes or packaging, or other materials originally sold with firearms, ammunition, or firearm accessories.

D. Photograph(s) of any firearm or ammunition, and firearms accessories.

E. Documents, ledgers, books, communications, or records relating to any firearm, ammunition, or firearm parts or accessories

F. Communications to or from any individual involved with the actual or contemplated possession, acquisition, purchase, storage, transportation, use, distribution, or sale of any firearm or ammunition.

G. Records evidencing the occupancy or use of the premises identified in Attachment A.

H. Records evidencing the identity of any individual who used or controlled the phone with number 617-818-8654, or the account associated with that phone number.

I. Records evidencing the identity of any individual who used or controlled the Instagram account associated with the profile “weezoskolo,” the Snapchat account associated with the profile “truwezechew,” the Snapchat account associated with the profile “weezoskolo,” and/or the Facebook account associated with www.facebook.com/chiweze.ihunwo.

J. Social media postings or other communications relating to any offer to buy or sell any firearms or ammunition.

K. Records evidencing the travel or whereabouts of Chiweze Ihunwo or any co-conspirators between October 2019 and the date of execution of the warrant.

L. Financial records including but not limited to, CashApp records, ApplePay records, and bank statements between October 2019 and the date of execution of the warrant.

M. United States currency in excess of $1,000.

N. Electronic devices including but not limited to computers, smartphones, cellular phones, GPS navigation units, and video surveillance systems.

O. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant (the computer equipment):

1. evidence of who used, owned, or controlled the computer equipment;
2. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;
3. evidence of the attachment of other computer hardware or storage media;
4. evidence of counter-forensic programs and associated data that are designed to eliminate data;
5. evidence of when the computer equipment was used;
6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage.

II. All computer hardware, computer software, and storage media owned or utilized by Chiweze IHUNWO or any other individual involved with the possession, acquisition, purchase, storage, transportation, use, distribution, or sale of any firearm, ammunition, or firearm

parts and/or accessories. Off-site searching of these items shall be limited to searching for the records described in paragraph I.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, mobile phone, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes